Aplicación de Visual Analytics para el análisis temporal de una dirección IP maliciosa en entornos de ciberseguridad

Mariños Hilario, Princce Yorwin

Orientador: Prof Dr./Mag./Ing. Nombre del Asesor

Plan de Tesis presentado la Escuela Profesional Ciencia de la Computación como paso previo a la elaboración de la Tesis Profesional.

UNSA - Universidad Nacional de San Agustín de Arequipa
Junio de 2025

Índice

1. Introducción

La digitalización ha transformado profundamente el funcionamiento de gobiernos, instituciones financieras y sectores estratégicos, pero también ha ampliado la superficie de exposición a ciberataques. Estas amenazas, cada vez más sofisticadas y persistentes, comprometen la estabilidad de infraestructuras críticas mediante técnicas que evolucionan en complejidad y escala [1, 2]. Frente a este escenario, las organizaciones recurren a los Centros de Operaciones de Seguridad (SOC). Los SOC son unidades especializadas que monitorean redes en tiempo real y responden ante incidentes mediante el análisis de grandes volúmenes de registros y alertas generadas por dispositivos de seguridad. Sin embargo, el incremento en la cantidad y frecuencia de eventos puede superar la capacidad de los analistas, provocando errores, omisiones y el fenómeno conocido como fatiga de alertas, que disminuye la eficacia de la respuesta operativa [3, 4]. La fatiga de alertas ocurre cuando los analistas son abrumados por un gran número de notificaciones de seguridad, lo que puede llevar a pasar por alto amenazas reales.

En este contexto, el análisis visual (también conocido como Visual Analytics) se ha consolidado como un enfoque efectivo dentro de la ciencia de datos aplicada a la ciberseguridad. Este método permite representar gráficamente la información para facilitar su interpretación, identificar relaciones temporales y semánticas en los datos, y acelerar los procesos de toma de decisiones [5, 6]. Su aplicación se ha demostrado útil en escenarios que requieren análisis forense, detección de anomalías y seguimiento de comportamiento malicioso, especialmente cuando los datos se presentan de forma interactiva y contextualizada [2].

Un concepto central en este trabajo es el de dirección IP maliciosa, que se refiere a un identificador numérico asignado a un dispositivo en una red, el cual ha sido vinculado a actividades perjudiciales o sospechosas, tales como escaneo de puertos (técnica utilizada para descubrir servicios abiertos en otros equipos), intentos de acceso no autorizado a sistemas, propagación de malware (programas diseñados para causar daño) o participación en redes de botnets (conjuntos de dispositivos comprometidos que actúan coordinadamente para realizar ataques) [7, 4]. Para estudiar estos comportamientos, se emplea tráfico de red etiquetado, es decir, datos de conexión que han sido previamente clasificados como benignos o maliciosos. Esta categorización es fundamental para entrenar y evaluar modelos de detección automatizada de amenazas. Uno de los recursos más utilizados para estos fines es el conjunto de datos CICIDS 2017, una colección pública que simula condiciones realistas con distintos tipos de ataques registrados en un entorno controlado [8]. El análisis de este tipo de información permite no solo identificar eventos aislados, sino también reconocer patrones de ataque, entendidos como comportamientos repetitivos y sistemáticos, y secuencias multietapa, que son campañas estructuradas en fases encadenadas —como reconocimiento, intrusión, persistencia y exfiltración— ejecutadas con distintos fines a lo largo del tiempo [9]. Asimismo, para facilitar el trabajo de análisis, se recurre a dashboards interactivos, es decir, interfaces visuales que permiten explorar los datos de forma dinámica e intuitiva. Estos paneles pueden incluir herramientas como líneas de tiempo, que representan eventos ordenados minuto a minuto, y mapas de calor (heatmaps), que destacan gráficamente los momentos de mayor intensidad de actividad, facilitando así la

detección de comportamientos anómalos o persistentes.

A pesar del avance de estas soluciones, la literatura especializada señala una limitación relevante: no existen herramientas enfocadas exclusivamente en visualizar, de forma integrada y eficiente, el comportamiento de una única dirección IP sospechosa [5, 10, 11]. Muchos de los sistemas actuales presentan vistas fragmentadas, por ejemplo, cronologías simples o visualizaciones de tráfico general sin una integración que permita un análisis puntual, ágil y contextualizado [12, 13, 14]. Esta falta de integración ralentiza el proceso de análisis, dificulta la identificación de patrones complejos y limita la capacidad de anticipación de los equipos de seguridad, contribuyendo a la ya mencionada fatiga de alertas.

Frente a esta problemática, el presente trabajo tiene como objetivo diseñar e implementar una interfaz interactiva para el análisis visual del tráfico de red asociado a una dirección IP maliciosa específica. La herramienta combinará una representación cronológica por minuto y un mapa de calor horario que permita identificar patrones de persistencia o secuencias multietapa en menos de 60 segundos, disminuyendo en al menos un 70 % el tiempo de análisis en comparación con métodos tradicionales basados en tablas. Con ello, se busca mejorar la eficiencia operativa en los SOC y optimizar la capacidad de respuesta.

2. Descripción del Dataset

El dataset *CICIDS2017* es un conjunto de datos especializado en el análisis de ciberseguridad, particularmente enfocado en la detección de tráfico malicioso dentro de redes informáticas. Fue diseñado para simular un entorno realista donde se registran sesiones de conexión tanto benignas como maliciosas, lo que permite entrenar y evaluar sistemas de detección de intrusos. Este dataset es ampliamente utilizado en la investigación de amenazas avanzadas, ya que contiene más de 80 características extraídas de flujos de red capturados mediante herramientas como *CICFlowMeter*.

Cada fila del dataset representa un flujo de conexión entre dos extremos (cliente-servidor), incluyendo variables como duración, número de paquetes, tamaños, tasas de envío, estadísticas temporales, indicadores de banderas TCP y, finalmente, una etiqueta que indica si el flujo es benigno o pertenece a un tipo específico de ataque (DoS, PortScan, BruteForce, entre otros). Esto permite realizar análisis supervisados y no supervisados en el ámbito de la detección de amenazas.

Cuadro 1: Resumen de técnicas aplicadas al dataset *CICIDS2017*

Técnica aplicada	**Descripción**	**Variables involucradas**	**Valor que aporta**
Preprocesamiento de datos	Limpieza de valores nulos, conversión de tipos, detección de outliers y duplicados	Todas las variables	Asegura consistencia y evita errores durante el análisis o modelado
Clasificación de tipos de datos	Identificación de variables continuas, discretas y categóricas	Todas las columnas	Permite aplicar métodos estadísticos adecuados a cada tipo de dato
Análisis estadístico	Cálculo de media, desviación estándar, mediana, moda, correlación y covarianza	Variables numéricas	Facilita la identificación de patrones y relaciones entre características
Análisis de balance de clases	Exploración de la variable *Label* para evaluar la distribución de etiquetas	Label	Detecta desequilibrios entre tráfico benigno y malicioso
Tratamiento de valores nulos	Eliminación o imputación de registros con valores nulos en columnas clave	Flow Bytes/s, Packet Length Mean, etc.	Evita distorsión en las métricas y errores en el modelado
Distribución temporal y granularidad	Evaluación de timestamps para identificar variaciones temporales y estacionales	Timestamp, Flow Duration	Permite detectar tendencias y variabilidad en diferentes períodos temporales
Extracción de features relevantes	Selección de columnas más representativas para el análisis	Variables correlacionadas con *Label*	Optimiza el rendimiento y la interpretabilidad en modelos de detección

3. Preguntas

El dataset CICIDS2017 contiene datos de tráfico de red con más de 80 variables para analizar tráfico benigno y ataques (DoS, PortScan, BruteForce, etc.).

Variables clave usadas en el análisis:

- **Flow Duration:** duración del flujo de conexión (importante para medir tiempo activo).
- **Fwd IAT Total y Bwd IAT Total:** tiempos entre paquetes enviados hacia adelante y hacia atrás (clave para distinguir tipos de tráfico).
- **Label:** clase que indica si el flujo es benigno o malicioso.
- **Timestamp:** marca temporal para análisis de tendencias y comportamientos temporales.

Este contexto ayuda a entender cómo se comporta el tráfico y qué variables son críticas para detectar ataques.

4. Problemas identificados en el dataset CICIDS2017

- Desbalance extremo en la variable `Label`: 98 % benigno, menos del 2 % ataques.
- Presencia de valores negativos erróneos en `Flow Duration`, corregidos para evitar distorsión.
- Muchas variables con alta proporción de ceros o datos faltantes (flags TCP, métricas bulk), descartadas por falta de información.

5. Descubrimientos al analizar los datos

- Variables temporales como `Flow Duration`, `Fwd IAT Total` y `Bwd IAT Total` están altamente correlacionadas, mostrando que la duración y tiempos entre paquetes son factores clave.
- Variables con poca o ninguna variabilidad fueron descartadas.
- El análisis estadístico y gráfico confirma diferencias claras entre tráfico benigno y malicioso.

6. Patrones de tendencia detectados

- El análisis de la variable `Flow Duration` a lo largo del tiempo muestra fluctuaciones significativas según la hora del día.
- Esto sugiere la existencia de picos de actividad relacionados con el comportamiento humano o ataques programados.
- El uso del campo `Timestamp` permitió hacer un análisis temporal agregando los datos por hora.

7. Comportamiento humano y movilidad en relación con la geografía

En este dataset, no contamos con datos geográficos explícitos, pero podemos usar atributos como `Protocolo`, `Puertos de destino` y `Horario` para inferir patrones de actividad humana en la red.

Los gráficos muestran que el tráfico varía según protocolo y puerto, y que la actividad maliciosa tiene horarios específicos, reflejando comportamientos planificados o estacionales.

Referencias

[1] Z. Liu, R. J. Crouser, and A. Ottley, "Survey on individual differences in visualization," *Computer Graphics Forum*, vol. 39, no. 3, pp. 693–712, 2020.

[2] K. Wang, S. Liu, W. Chen, C. North, and H. Qu, "Timelinesec: Interactive visual analytics for multivariate cyber-security event sequences," *IEEE Transactions on Visualization and Computer Graphics*, 2020.

[3] M.-H. M. Chung, Y. A. Yang, L. Wang, G. Cento, K. Jerath, P. Taank, A. Raman, J. H. Chan, and M. H. Chignell, "Enhancing cybersecurity situation awareness through visualization: A usb data-exfiltration case study," *Heliyon*, vol. 9, no. 1, p. e16232, 2023.

[4] H. N. Nguyen, F. Abri, V. V. Pham, M. Chatterjee, A. S. Namin, and T. Dang, "Malview: Interactive visual analytics for comprehending malware behavior," *IEEE Access*, vol. 10, pp. 99909–99930, 2022.

[5] X. Li, J. Chen, S. Wang, and X. Zhang, "Visual analytics for cyber-threat intelligence: A survey," *International Journal of Information Security*, vol. 22, no. 3, 2023.

[6] J. Zhao, L. Lee, and W. Zhang, "Dynamic visual analytics of host-based intrusion data," *Journal of Network and Computer Applications*, vol. 150, p. 102947, 2020.

[7] A. Alshamrani, J. Reed, and D. Chau, "Darknetscope: Visual analytics for dark web traffic investigation," *Digital Investigation*, vol. 41, p. 101129, 2022.

[8] I. Sharafaldin, A. M. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *CICIDS 2017 Proceedings*, pp. 108–116, 2018.

[9] S. Ayari, O. Ferchichi, and R. Boughammoura, "Masfad: Multi-stage attack forensics with anomaly-driven dashboards," in *2023 International Conference on Military Communications and Information Systems (ICMCIS)*, 2023.

[10] R. Mendez, C. Zhang, L. Wang, and T. Peng, "Chronocti: Time-aligned visualization for cyber-threat intelligence," in *Proceedings of the IEEE Symposium on Visualization for Cyber Security (VizSec 2024)*, 2024.

[11] Q. Ye, Y. Han, P. Du, and X. Li, "Decades: Decentralized event correlation and advanced detection system," *IEEE Access*, vol. 9, pp. 19535–19548, 2021.

[12] Z. Nedelkoski, M. Keck, M. Wiesner, and B. Richerzhagen, "Flowscope: Visual root-cause analysis for large-scale network management," in *2021 IEEE Conference on Network and Service Management (CNSM)*, pp. 294–300, 2021.

[13] A. Delacroix, J. Bruneau, and L. Lemaire, "Aptvis: Interactive visualization of advanced persistent threat campaigns," in *VizSec 2023*, 2023.

[14] D. H. Jeong, J.-H. Cho, F. Chen, L. Kaplan, A. Jøsang, and S.-Y. Ji, "Interactive web-based visual analysis on network traffic data," *Information*, vol. 14, no. 1, p. 16, 2023.